Considerations for STA Traffic Mirroring

Product Version	3.0.64C and above
Document Version	v1.0
Released on	2023-05-06

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

Intended Audience

This document is intended for:

- Pre-sales
- FAE

Note Icons

English Icon	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
⚠ NOTICE	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
📖 NOTE	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
2023-05-06	This is the first release of this document.

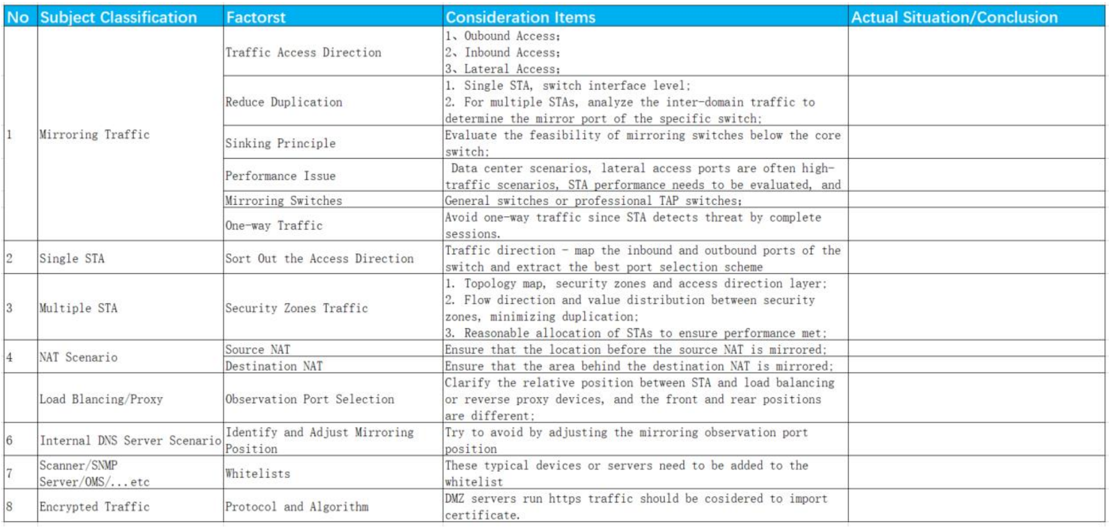
Contents

1 Overall Description

Different from gateway products (such as WAF, AF, IPS, etc.), CC products themselves are platform products, and STA is deployed in a bypass. The installation and deployment will not affect the customer's network, and only need to configure mirroring on the switch, so It is easy to get started, but what needs to be paid attention to is that before deployment, research on special typical scenarios (such as: NAT scenarios, load/proxy scenarios, DNS server scenarios, etc.)

A summary of the content is shown in the attached table below:

overall considerations.xls

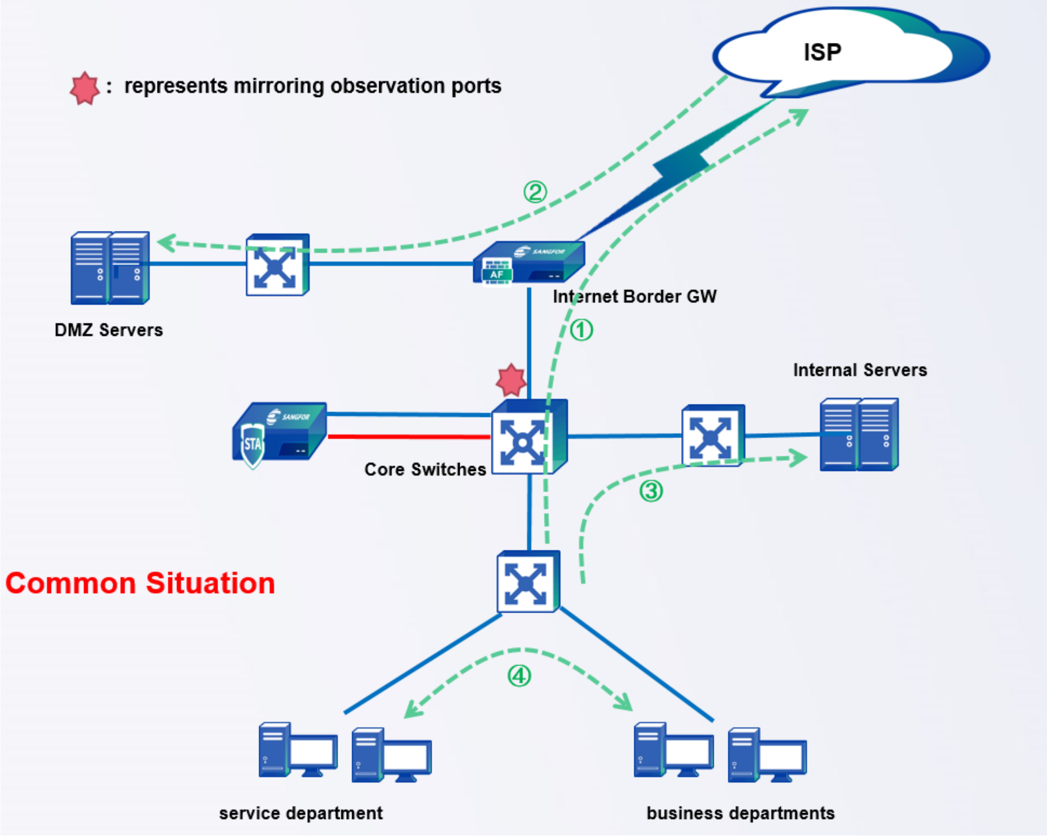


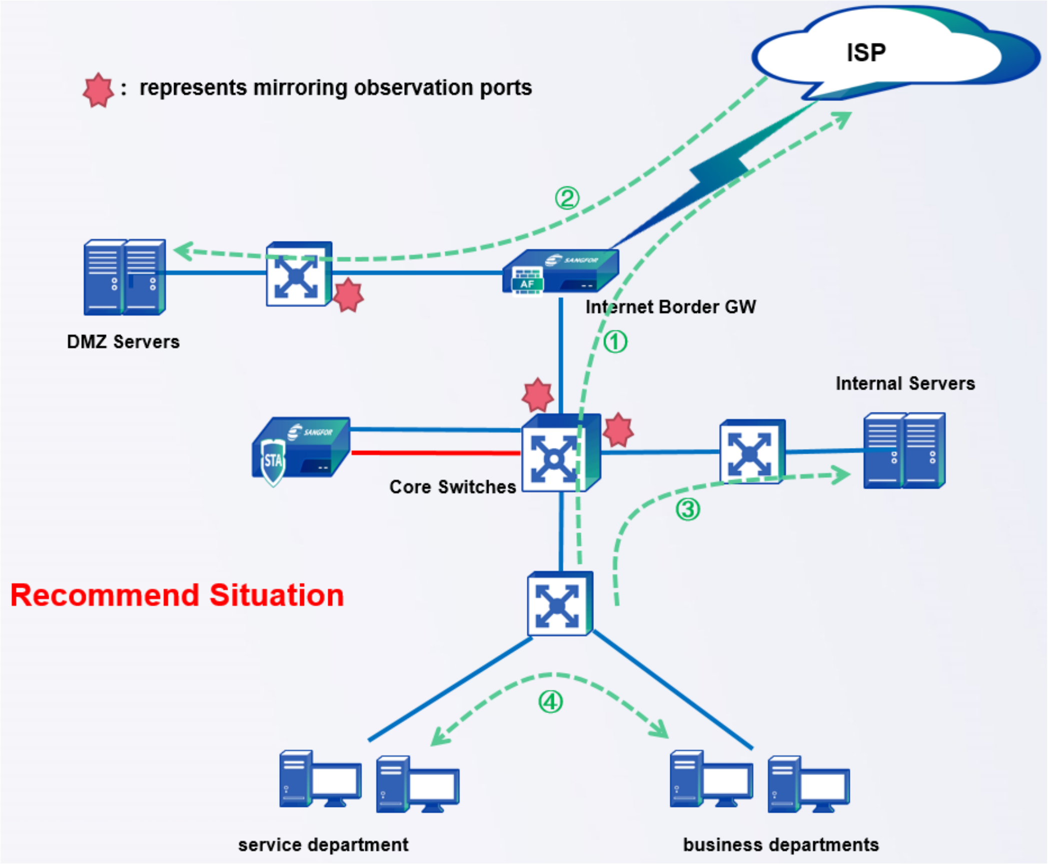
No	Subject Classification	Factorst	Consideration Items	Actual Situation/Conclusion

1	Mirroring Traffic	Traffic Access Direction	1、Oubound Access;
			2、Inbound Access;
			3、Lateral Access;	

		Reduce Duplication	1. Single STA, switch interface level; 2. For multiple STAs, analyze the inter-domain traffic to determine the mirror port of the specific switch;	
		Sinking Principle	Evaluate the feasibility of mirroring switches below the core switch;	
		Performance Issue	Data center scenarios, lateral access ports are often high-traffic scenarios, STA performance needs to be evaluated, and	
		Mirroring Switches	General switches or professional TAP switches;	
		One-way Traffic	Avoid one-way traffic since STA detects threat by complete sessions.	
2	Single STA	Sort Out the Access Direction	Traffic direction - map the inbound and outbound ports of the switch and extract the best port selection scheme	
3	Multiple STA	Security Zones Traffic	1. Topology map, security zones and access direction layer; 2. Flow direction and value distribution between security zones, minimizing duplication; 3. Reasonable allocation of STAs to ensure performance met;	
4	NAT Scenario	Source NAT	Ensure that the location before the source NAT is mirrored;	
		Destination NAT	Ensure that the area behind the destination NAT is mirrored;	
	Load Blancing/Proxy	Observation Port Selection	Clarify the relative position between STA and load balancing or reverse proxy devices, and the front and rear positions are different;	
6	Internal DNS Server Scenario	Identify and Adjust Mirroring Position	Try to avoid by adjusting the mirroring observation port position	
7	Scanner/SNMP Server/OMS/...etc	Whitelists	These typical devices or servers need to be added to the whitelist	
8	Encrypted Traffic	Protocol and Algorithm	DMZ servers run https traffic should be cosidered to import certificate.	

- **Traffic Direction**: In principle,outbound access, inbound access, and lateral access,mirroring traffic is performed based on these three flows from the perspective of direction, among which outbound access is mainly terminal or server access Internet traffic, inbound access mainly refers to the access of Internet users to external servers, lateral access mainly refers to cross-security zones communication from terminal to terminal or internal server, branches access HQ through leased line/VPN in branch scenarios, etc... When conduct mirroring policy,we give priority to ensuring the direction of outbound access and inbound access. As for lateral access, we try to cover it as much as possible.


: represents mirroring observation ports
ISP
②
DMZ Servers
Internet Border GW
①
Internal Servers
Core Switches
③
STA
AF
Common Situation
④
service department
business departments

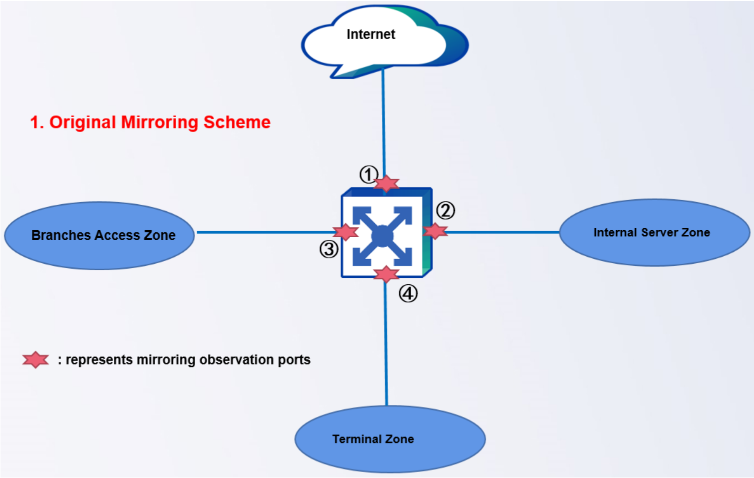

: represents mirroring observation ports
ISP
②
DMZ Servers
Internet Border GW
①
Internal Servers
Core Switches
③
STA
AF
Recommend Situation
④
service department
business departments

- **Reduce Duplication:** In a multi-domain network environment, it is easy to cause traffic duplication. It is necessary to delineate and discuss the working scope of each STA to avoid highly repetitive traffic situations.
- **Sinking Principle**: Theoretically, traffic mirroring should sink as far as possible to peripheral areas, such as traffic before mirroring to DHCP server,DNS server and other servers, which will make subsequent security operations much more convenient.
- **Performance Issues**: For example, in a data center scenario, internal links are often at the 10GE level,and lateral access traffic is much larger than inbund access traffic. In this case, it is necessary to evaluate whether the performance of the STA can support lateral access traffic.
- **Mirroring Switches**: For some industry customers, even if only mirroring the outbound traffic from core switches is too large, a single STA cannot handle it. In this case, it is necessary to improve the STA model, and on the other hand, use a TAP switch to offload the mirroring to each STA.
- **One-way Traffic**: STA analyzes based on complete sessions. When conduct mirroring policy, it is necessary to ensure the integrity of the request traffic and response traffic. Avoid that only request traffic or only response traffic is mirrored since STA will not analysis in most occasions
- **Typical Devices**: Such as NAT、DNS、SNMP、OMS、Scanner devices...etc,should be taken into consideration respectively(see the details in following chapters).

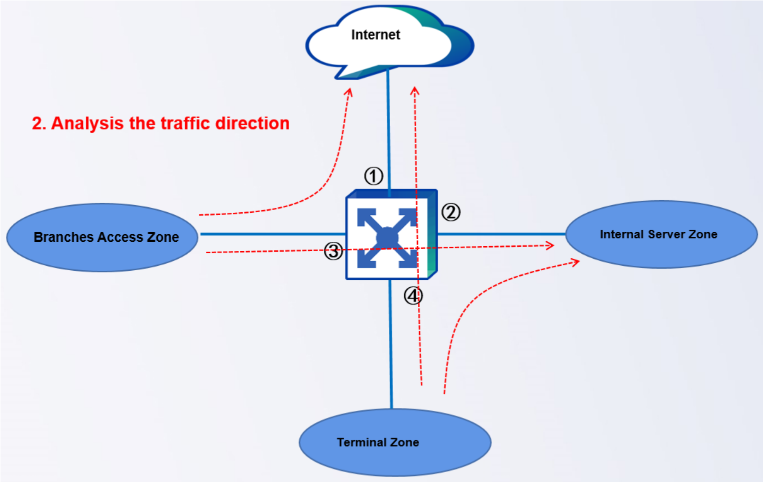
2 Single STA situation

Take the switch interface as the unit and analyze the internal areas traffic to determine the minimum number or optimum combination of mirroring observation ports that need to be mirrored.

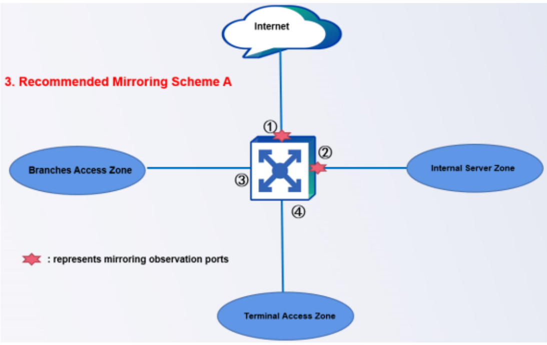
Example: core switch interfaces ①②③④ link to four areas respectively, the orginal mirroring policy is that all the 4 ports are mirrored as shown in below diagram.

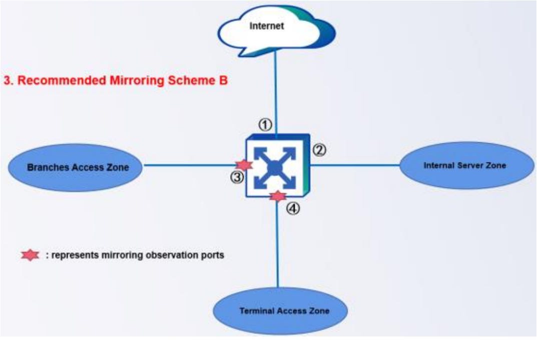

Internet
1. Original Mirroring Scheme
①
②
③
④
Branches Access Zone
Internal Server Zone
: represents mirroring observation ports
Terminal Zone

Analysis and draw the access direction we will check out duplicated traffic.



Then we will conclude the exact ports which need to be mirrored.


Internet
3. Recommended Mirroring Scheme A
①
②
③
④
Branches Access Zone
Internal Server Zone
: represents mirroring observation ports
Terminal Access Zone


Internet
3. Recommended Mirroring Scheme B
①
②
③
④
Branches Access Zone
Internal Server Zone
: represents mirroring observation ports
Terminal Access Zone

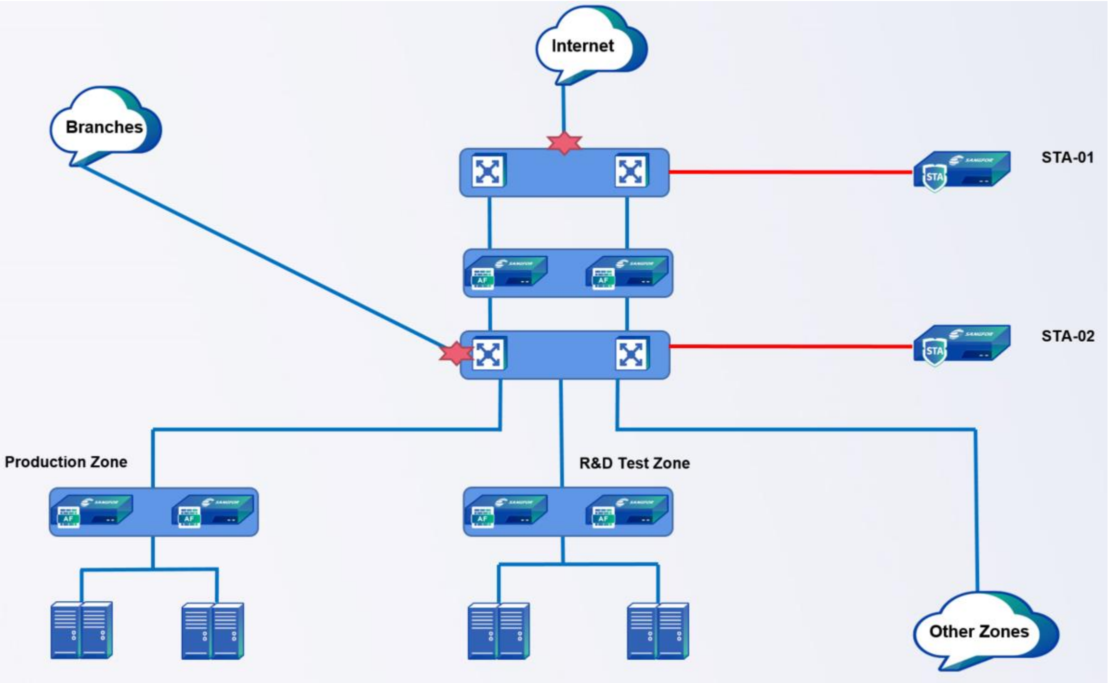
3 Multiple STA

In fact, it is common to see multiple STAs in customer's network. If they are deployed at will, duplicated traffic will increase the number of logs and increase unnecessary resource consumption for STAs. The scope of action of a single STA should be clear, and the crossover should be reduced as much as possible. Below diagram is an actual deployment of a customer as an example. The problems including:

1. Mirroring the traffic after source NAT;

2. Some key zones like Production Zone and R&D Test Zone are not covered and the capability of STA are not be taken full use;

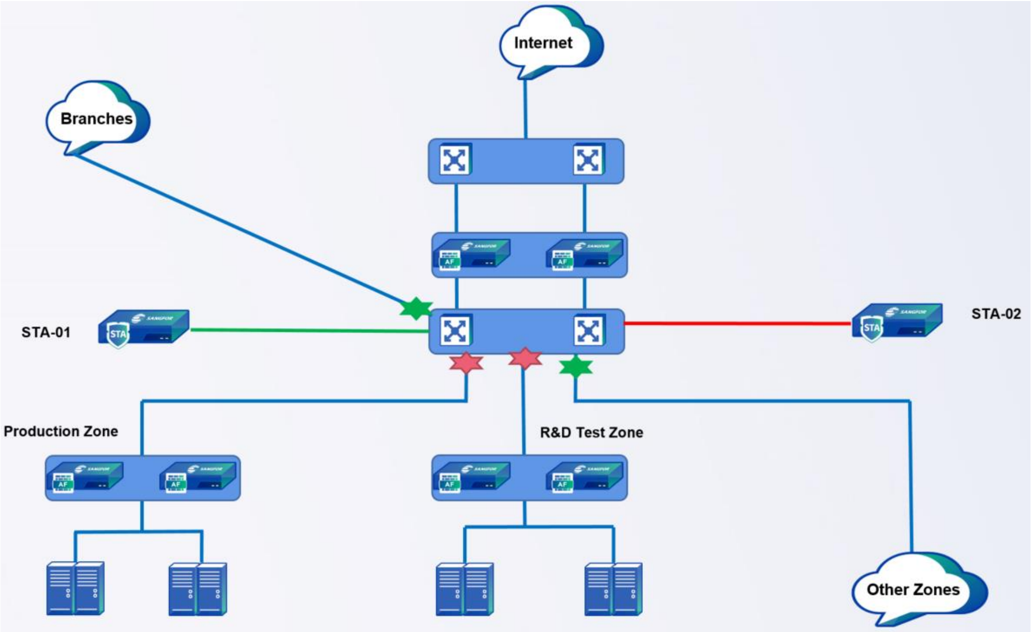
3. There are some duplicated traffic between STA-01 and STA-02;



After analysis of problems, we can adjust the deployment position as below.

The STA-01 can cover Branches and Other Zones to detect threats.

The STA-02 can cover Production and R&D Test Zones to detect threats.

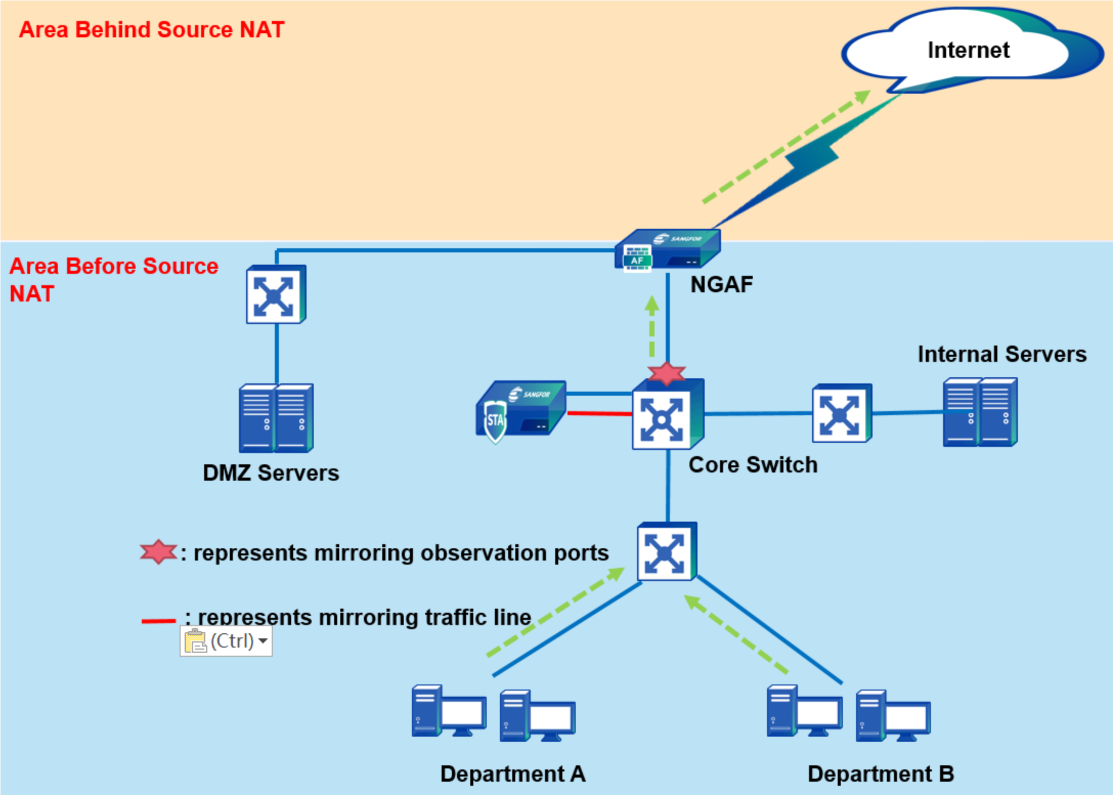


4 NAT Scenario

There are mainly 3 types of NAT, they are source NAT、destination NAT and two-way NAT. For two-way NAT scenarios, there is no good way to do correlation analysis of before and after NAT device since both source IP and destination IP are replaced at the same time.

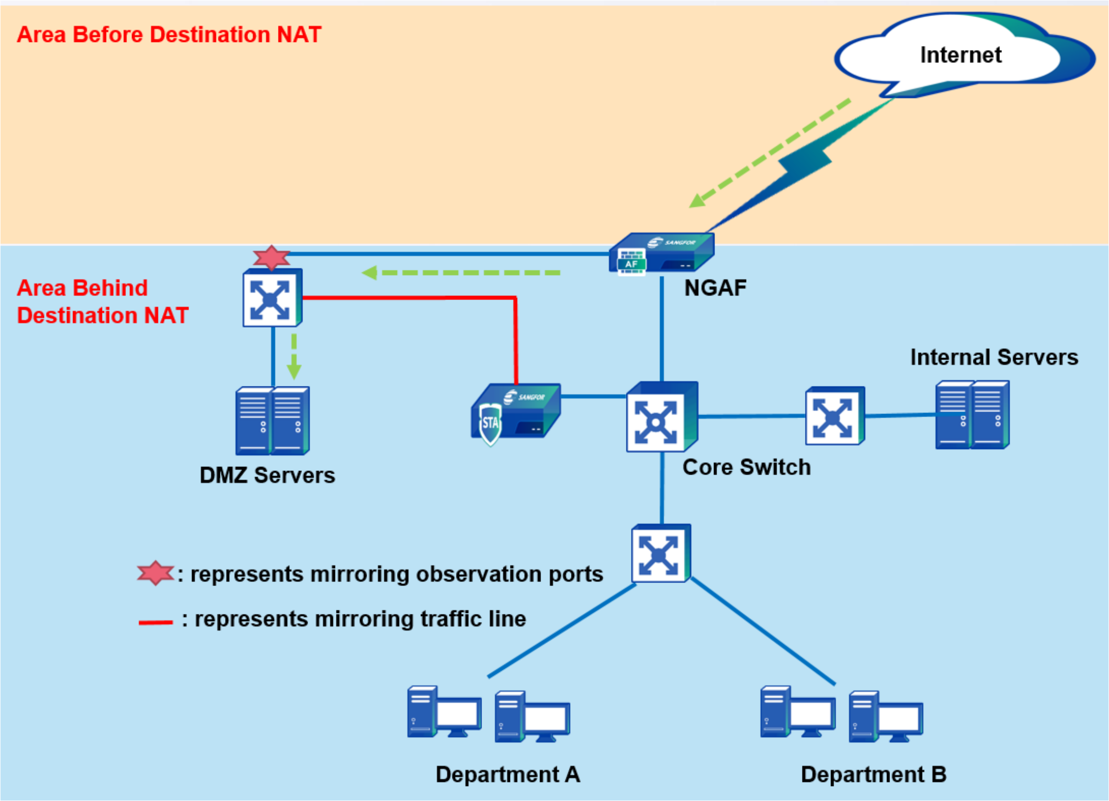
4.1 Source NAT

Make sure that mirroring traffic area locates before source NAT.



4.2 Destination NAT

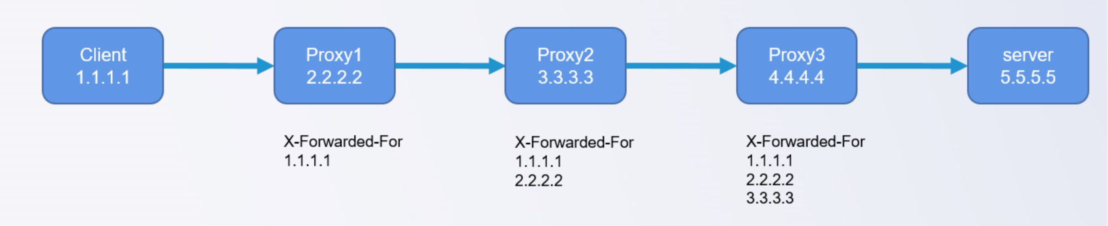
Make sure that mirroring traffic area locates behind destination NAT.


Area Before Destination NAT
Internet
Area Behind Destination NAT
NGAF
Internal Servers
DMZ Servers
Core Switch
: represents mirroring observation ports
: represents mirroring traffic line
Department A
Department B

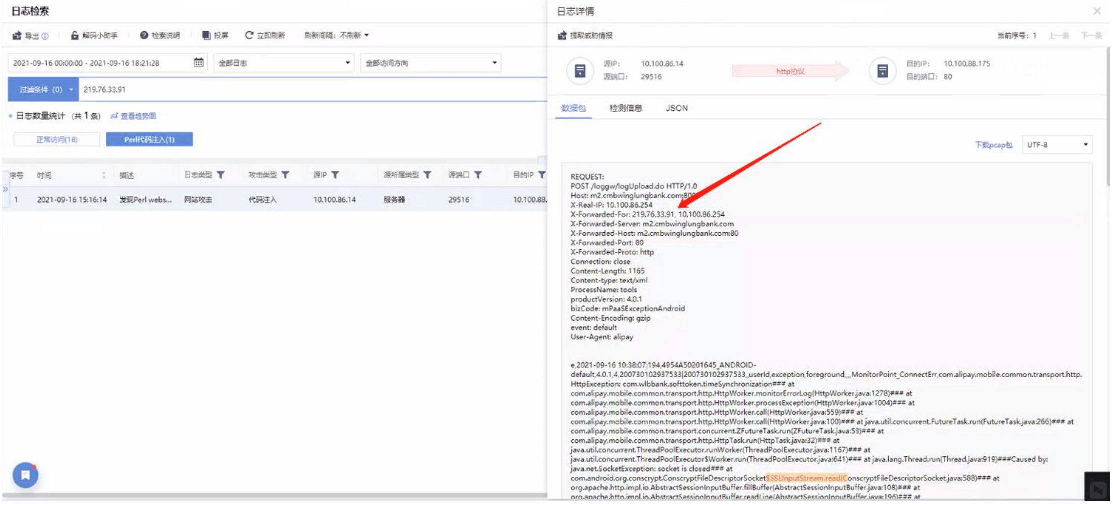
5 Load Blancing/Proxy Scenario

5.1 Basic Understanding

In a multi-level proxy, X-Forwarded-For in the http request header is used to record all proxy addresses from the client address to the last proxy server, as shown below.



When tracing the attacker source IP, usually the first IP address in the X-Forwarded-For field is the real client address. As shown in the screenshot below, after two layers of proxy, the real source IP is: 219.76.33.91, the first layer of proxy: 10.100.86.254, the second layer of proxy: 10.100.86.14



2021-09-16 00:00:00 - 2021-09-16 18:21:28

219.76.33.91

日志数量统计（共 1 条）

序号	时间	描述	日志类型	攻击类型	源IP	源所属类型	源端口	目的IP
1	2021-09-16 15:16:14	发现Perl webs...	网站攻击	代码注入	10.100.86.14	服务器	29516	10.100.88.

当前序号：1

源IP： 10.100.86.14
源端口： 29516

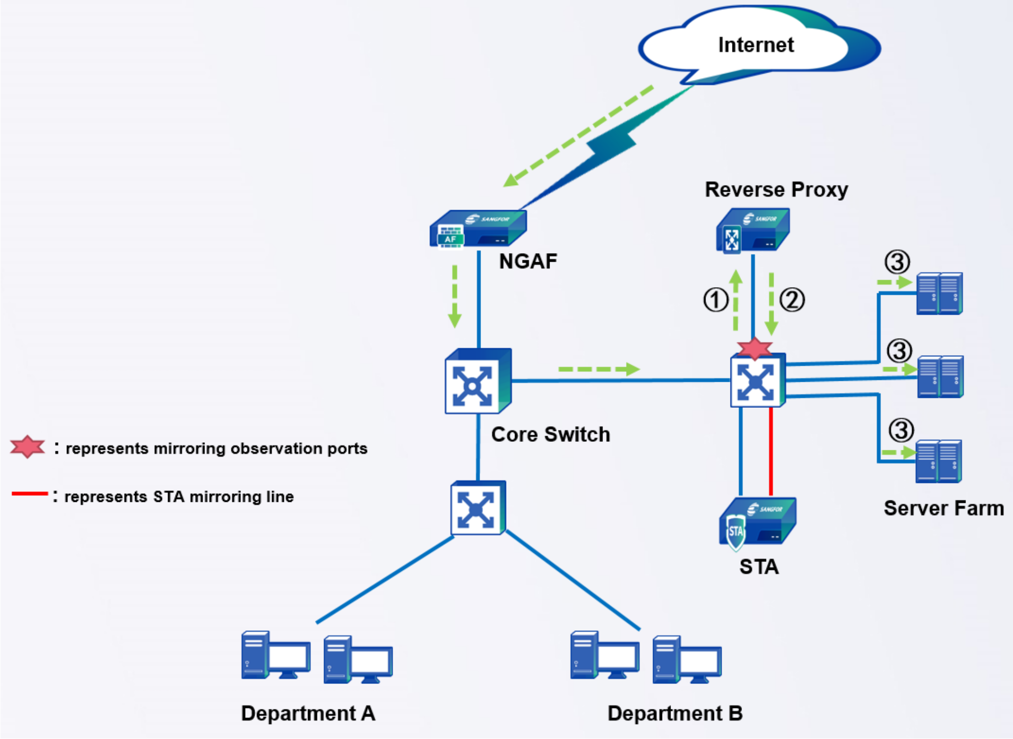
目的IP： 10.100.88.175
目的端口： 80

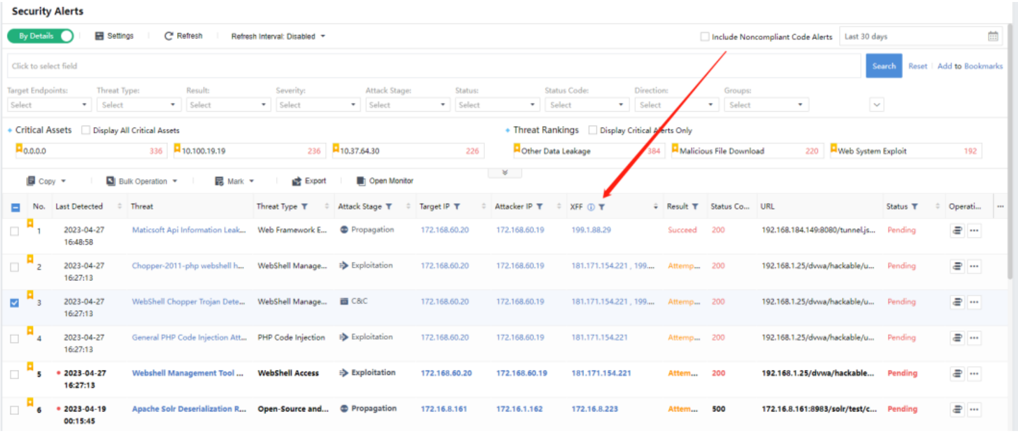
```
REQUEST:
POST /loggw/logUpload.do HTTP/1.0
Host: m2.cmbwinglungbank.com:80
X-Real-IP: 10.100.86.254
X-Forwarded-For: 219.76.33.91, 10.100.86.254
X-Forwarded-Server: m2.cmbwinglungbank.com
X-Forwarded-Host: m2.cmbwinglungbank.com:80
X-Forwarded-Port: 80
X-Forwarded-Proto: http
Connection: close
Content-Length: 1165
Content-type: text/xml
ProcessName: tools
productVersion: 4.0.1
bizCode: mPaaSExceptionAndroid
Content-Encoding: gzip
event: default
User-Agent: alipay


e,2021-09-16 10:38:07:194,4954A50201645_ANDROID-
default,4.0.1,4,200730102937533|200730102937533,,userId,exception,foreground,,,,MonitorPoint_ConnectErr,com.alipay.mobile.common.transport.http.
HttpException: com.wlbbank.softtoken.timeSynchronization### at
com.alipay.mobile.common.transport.http.HttpWorker.monitorErrorLog(HttpWorker.java:1278)### at
com.alipay.mobile.common.transport.http.HttpWorker.processException(HttpWorker.java:1004)### at
com.alipay.mobile.common.transport.http.HttpWorker.call(HttpWorker.java:559)### at
com.alipay.mobile.common.transport.http.HttpWorker.call(HttpWorker.java:100)### at java.util.concurrent.FutureTask.run(FutureTask.java:266)### at
com.alipay.mobile.common.transport.concurrent.ZFutureTask.run(ZFutureTask.java:53)### at
com.alipay.mobile.common.transport.http.HttpTask.run(HttpTask.java:32)### at
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1167)### at
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:641)### at java.lang.Thread.run(Thread.java:919)###Caused by:
java.net.SocketException: socket is closed### at
com.android.org.conscrypt.ConscryptFileDescriptorSocket$SSLInputStream.read(ConscryptFileDescriptorSocket.java:588)### at
org.apache.http.impl.io.AbstractSessionInputBuffer.fillBuffer(AbstractSessionInputBuffer.java:108)### at
org.apache.http.impl.io.AbstractSessionInputBuffer.readLine(AbstractSessionInputBuffer.java:196)### at
```

5.2 Mirroring Observation Position

In reverse proxy scenario, it is recommended that you should deploy the STA mirroring traffic after reverse proxy server since CC can detect x-forward-for field and we can see it in security alerts.




Security Alerts

By Details | Settings | Refresh | Refresh Interval: Disabled ▾ | □ Include Noncompliant Code Alerts | Last 30 days

Click to select field | Search | Reset | Add to Bookmarks

Target Endpoints: Select ▾ | Threat Type: Select ▾ | Result: Select ▾ | Severity: Select ▾ | Attack Stage: Select ▾ | Status: Select ▾ | Status Code: Select ▾ | Direction: Select ▾ | Groups: Select ▾

Critical Assets □ Display All Critical Assets

0.0.0.0 336 | 10.100.19.19 236 | 10.37.64.30 226

Threat Rankings □ Display Critical Alerts Only

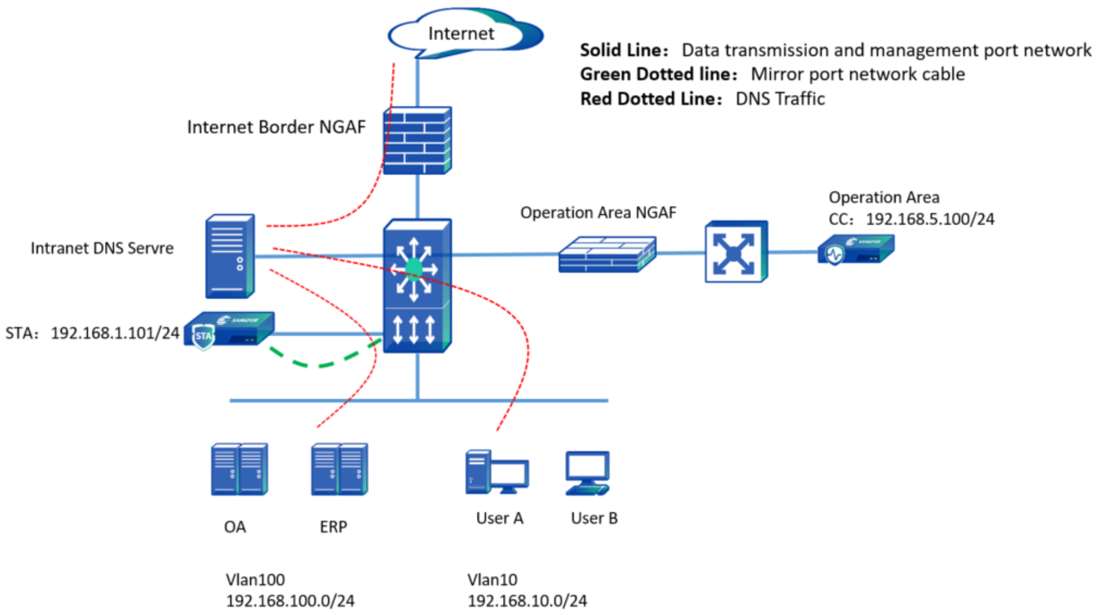
Other Data Leakage 384 | Malicious File Download 220 | Web System Exploit 192

Copy ▾ | Bulk Operation ▾ | Mark ▾ | Export | Open Monitor

	No.	Last Detected	Threat	Threat Type	Attack Stage	Target IP	Attacker IP	XFF	Result	Status Co...	URL	Status	Operati...
□	1	2023-04-27 16:48:58	Maticsoft Api Information Leak...	Web Framework E...	Propagation	172.168.60.20	172.168.60.19	199.1.88.29	Succeed	200	192.168.184.149:8080/tunnel.js...	Pending	⋯
□	2	2023-04-27 16:27:13	Chopper-2011-php webshell h...	WebShell Manage...	Exploitation	172.168.60.20	172.168.60.19	181.171.154.221 , 199....	Attemp...	200	192.168.1.25/dvwa/hackable/u...	Pending	⋯
☑	3	2023-04-27 16:27:13	WebShell Chopper Trojan Dete...	WebShell Manage...	C&C	172.168.60.20	172.168.60.19	181.171.154.221 , 199....	Attemp...	200	192.168.1.25/dvwa/hackable/u...	Pending	⋯
□	4	2023-04-27 16:27:13	General PHP Code Injection Att...	PHP Code Injection	Exploitation	172.168.60.20	172.168.60.19	181.171.154.221	Attemp...	200	192.168.1.25/dvwa/hackable/u...	Pending	⋯
□	5	2023-04-27 16:27:13	Webshell Management Tool ...	WebShell Access	Exploitation	172.168.60.20	172.168.60.19	181.171.154.221	Attem...	200	192.168.1.25/dvwa/hackable...	Pending	⋯
□	6	2023-04-19 00:15:45	Apache Solr Deserialization R...	Open-Source and...	Propagation	172.16.8.161	172.16.1.162	172.16.8.223	Attem...	500	172.16.8.161:8983/solr/test/c...	Pending	⋯

6 Internal DNS Server Scenario

6.1 Scenario Description



The above network topology can illustrate intranet DNS Server scenarios in some customers' network structure. When STA receives the mirrored data that is the data behind the intranet DNS server, it will judge the DNS server as a risky host, and cannot locate the real problem business.

6.2 From Logs to Infer Mirroring Policy

There are three conditions from which you can infer the location of the mirrored traffic related to the intranet DNS server.

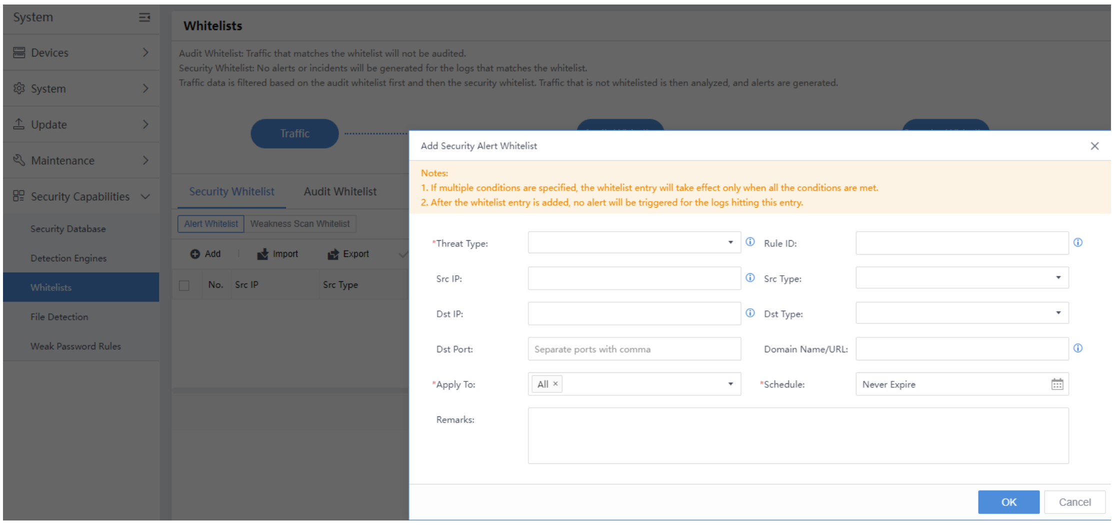
Case 1: Check the DNS logs in CC platform. If the intranet DNS server IP is both the source and the destination in logs, it means that the traffic before and after the DNS server are all mirrored. You have to add DNS server into security whitelist as the source address and it is necessary to modify the traffic policy.

Case 2: Check the DNS logs in CC platform. If the intranet DNS server IP is only the destination address, it means that the mirrored traffic is the traffic before the DNS server, and the mirroring is correct. There is nothing to modify.

Case 3: Check the DNS logs in CC platform. If the the intranet DNS server is only the source address, it means that the mirrored traffic is only after the DNS server, in which condition you can not tell the real problematic terminals . In this case, you need to mirror the right traffic by changing the location of observation port.

7 Scanner/SNMP/OMS Scenario

These typical devices will lead to some misjudgement in CC if you do not intervene. We recommend that you should add them into whitelists during the period of deployment.



Whitelists

Audit Whitelist: Traffic that matches the whitelist will not be audited.
Security Whitelist: No alerts or incidents will be generated for the logs that matches the whitelist.
Traffic data is filtered based on the audit whitelist first and then the security whitelist. Traffic that is not whitelisted is then analyzed, and alerts are generated.

Add Security Alert Whitelist

Notes:
1. If multiple conditions are specified, the whitelist entry will take effect only when all the conditions are met.
2. After the whitelist entry is added, no alert will be triggered for the logs hitting this entry.

*Threat Type:		Rule ID:	
Src IP:		Src Type:	
Dst IP:		Dst Type:	
Dst Port:	Separate ports with comma	Domain Name/URL:	
*Apply To:	All ×	*Schedule:	Never Expire
Remarks:			

8 Encrypted Traffic Consideration

Currently, the vast majority of important business systems communicates by HTTPS rather than HTTP protocal. The inbound access data will be invisible if the private keys of external servers are not imported in STA.

【Scope of Application】

Encryption protocol versions of TLS/SSL STA supports are:

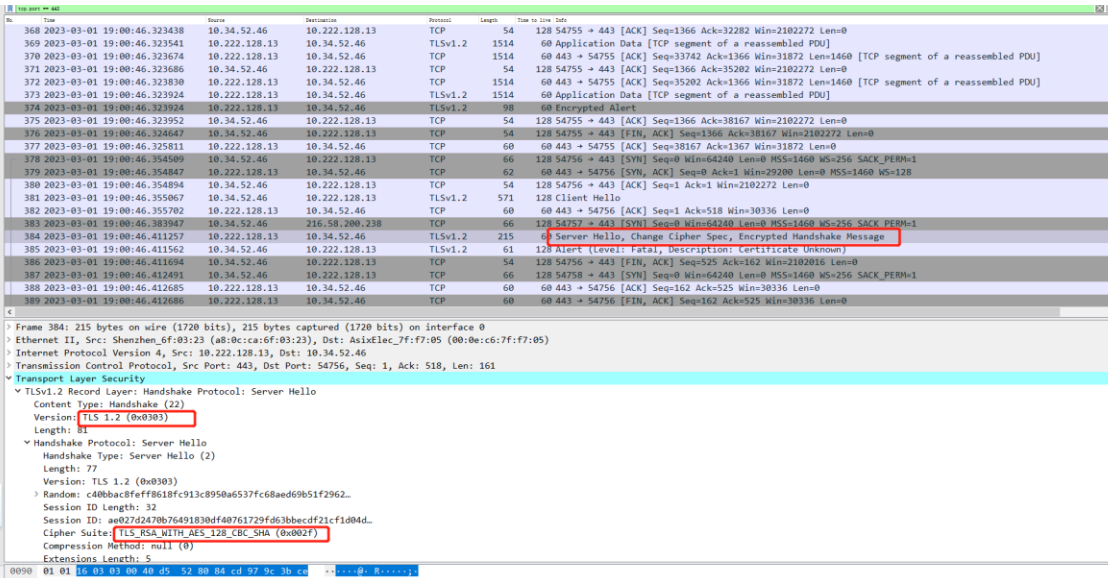
ssl 3.0、tls 1.0、tls 1.1、tls 1.2;

The algorithm STA supports are:

- **Symmetric algorithm**: DES, 3DES, AES are all supported;
- **Asymmetric algorithm**: RSA and ECDH are supported, but ECDHE is not supported;

How to distinguish what algorithm method the https traffic is?

We can check the server hello response content by capturing the https traffic packet.

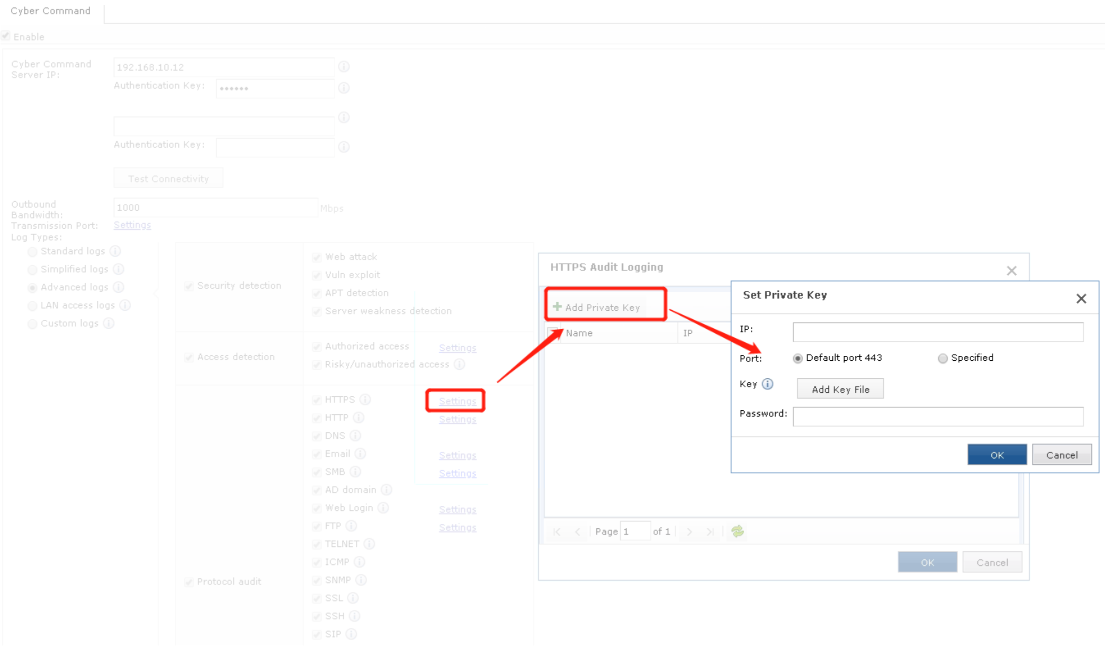


```
tcp.port == 443
No.  Time                          Source         Destination     Protocol  Length  Time to live Info
 368 2023-03-01 19:00:46.323438    10.34.52.46    10.222.128.13   TCP         54    128 54755 → 443 [ACK] Seq=1366 Ack=32282 Win=2102272 Len=0
 369 2023-03-01 19:00:46.323541    10.222.128.13  10.34.52.46     TLSv1.2   1514     60 Application Data [TCP segment of a reassembled PDU]
 370 2023-03-01 19:00:46.323674    10.222.128.13  10.34.52.46     TCP       1514     60 443 → 54755 [ACK] Seq=33742 Ack=1366 Win=31872 Len=1460 [TCP segment of a reassembled PDU]
 371 2023-03-01 19:00:46.323686    10.34.52.46    10.222.128.13   TCP         54    128 54755 → 443 [ACK] Seq=1366 Ack=35202 Win=2102272 Len=0
 372 2023-03-01 19:00:46.323830    10.222.128.13  10.34.52.46     TCP       1514     60 443 → 54755 [ACK] Seq=35202 Ack=1366 Win=31872 Len=1460 [TCP segment of a reassembled PDU]
 373 2023-03-01 19:00:46.323924    10.222.128.13  10.34.52.46     TLSv1.2   1514     60 Application Data [TCP segment of a reassembled PDU]
 374 2023-03-01 19:00:46.323924    10.222.128.13  10.34.52.46     TLSv1.2     98     60 Encrypted Alert
 375 2023-03-01 19:00:46.323952    10.34.52.46    10.222.128.13   TCP         54    128 54755 → 443 [ACK] Seq=1366 Ack=38167 Win=2102272 Len=0
 376 2023-03-01 19:00:46.324647    10.34.52.46    10.222.128.13   TCP         54    128 54755 → 443 [FIN, ACK] Seq=1366 Ack=38167 Win=2102272 Len=0
 377 2023-03-01 19:00:46.325811    10.222.128.13  10.34.52.46     TCP         60     60 443 → 54755 [ACK] Seq=38167 Ack=1367 Win=31872 Len=0
 378 2023-03-01 19:00:46.354509    10.34.52.46    10.222.128.13   TCP         66    128 54756 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 379 2023-03-01 19:00:46.354847    10.222.128.13  10.34.52.46     TCP         62     60 443 → 54756 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 WS=128
 380 2023-03-01 19:00:46.354894    10.34.52.46    10.222.128.13   TCP         54    128 54756 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
 381 2023-03-01 19:00:46.355067    10.34.52.46    10.222.128.13   TLSv1.2    571    128 Client Hello
 382 2023-03-01 19:00:46.355702    10.222.128.13  10.34.52.46     TCP         60     60 443 → 54756 [ACK] Seq=1 Ack=518 Win=30336 Len=0
 383 2023-03-01 19:00:46.383947    10.34.52.46    216.58.200.238  TCP         66    128 54757 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 384 2023-03-01 19:00:46.411257    10.222.128.13  10.34.52.46     TLSv1.2    215     60 Server Hello, Change Cipher Spec, Encrypted Handshake Message
 385 2023-03-01 19:00:46.411562    10.34.52.46    10.222.128.13   TLSv1.2     61    128 Alert (Level: Fatal, Description: Certificate Unknown)
 386 2023-03-01 19:00:46.411694    10.34.52.46    10.222.128.13   TCP         54    128 54756 → 443 [FIN, ACK] Seq=525 Ack=162 Win=2102016 Len=0
 387 2023-03-01 19:00:46.412491    10.34.52.46    10.222.128.13   TCP         66    128 54758 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 388 2023-03-01 19:00:46.412685    10.222.128.13  10.34.52.46     TCP         60     60 443 → 54756 [ACK] Seq=162 Ack=525 Win=30336 Len=0
 389 2023-03-01 19:00:46.412686    10.222.128.13  10.34.52.46     TCP         60     60 443 → 54756 [FIN, ACK] Seq=162 Ack=525 Win=30336 Len=0

> Frame 384: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
> Ethernet II, Src: Shenzhen_6f:03:23 (a8:0c:ca:6f:03:23), Dst: AsixElec_7f:f7:05 (00:0e:c6:7f:f7:05)
> Internet Protocol Version 4, Src: 10.222.128.13, Dst: 10.34.52.46
> Transmission Control Protocol, Src Port: 443, Dst Port: 54756, Seq: 1, Ack: 518, Len: 161
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 81
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 77
        Version: TLS 1.2 (0x0303)
      > Random: c40bbac8feff8618fc913c8950a6537fc68aed69b51f2962…
        Session ID Length: 32
        Session ID: ae027d2470b76491830df40761729fd63bbecdf21cf1d04d…
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Compression Method: null (0)
        Extensions Length: 5
0090  01 01 16 03 03 00 40 d5  52 80 84 cd 97 9c 3b ce   ······@· R·····;·
```

Where to import the private key in STA if it is in the scope of application?

Navigate: System->Cyber Command



Cyber Command

☑ Enable

Cyber Command Server IP: 192.168.10.12

Authentication Key: ••••••

Authentication Key:

Test Connectivity

Outbound Bandwidth: 1000 Mbps

Transmission Port: Settings

Log Types:

○ Standard logs
○ Simplified logs
● Advanced logs
○ LAN access logs
○ Custom logs

☑ Security detection: ☑ Web attack, ☑ Vuln exploit, ☑ APT detection, ☑ Server weakness detection

☑ Access detection: ☑ Authorized access (Settings), ☑ Risky/unauthorized access

☑ Protocol audit: ☑ HTTPS (Settings), ☑ HTTP (Settings), ☑ DNS, ☑ Email (Settings), ☑ SMB (Settings), ☑ AD domain, ☑ Web Login (Settings), ☑ FTP (Settings), ☑ TELNET, ☑ ICMP, ☑ SNMP, ☑ SSL, ☑ SSH, ☑ SIP

HTTPS Audit Logging

+ Add Private Key

Name | IP

Page 1 of 1

OK Cancel

Set Private Key

IP:

Port: ● Default port 443 ○ Specified

Key: Add Key File

Password:

OK Cancel

WARNING

Be careful, as it is a software decryption for STA, not a hardware decryption card, it will consume a amount of STA resources and reduce efficiency.

9 Index

9.1 Communication Ports

Domain Name/ Destination IP address	**Ports**	**Function**
CC's IP address is 443, 4430, or 4488.	443(TCP),4430(TCP),4488(TCP)	CC's 443 and 4430 ports are for STA to sync logs to CC. CC's 4488 port is for STA to send a database update request to CC.
CC's IP address is 4430. NGAF IP address's 7443.	4430(TCP),7443(TCP)	CC's 4430 port is for NGAF to sync log to CC. NGAF's 7443 port is for CC to push integration action to NGAF.
CC's IP address is 7443. ES's IP address is 443.	4430(TCP), 7443(TCP)	CC's 7443 port is for ES to sync log to CC. ES's 443 port is for CC to push integration action to ES.
IAG's IP address is 7443 or 9998. CC's IP address is 1775 or 7443.	7443(TCP), 9998(TCP), 1775 (UDP)	IAG's 7443 and 9998 ports are for CC to push integration action to IAG. IAG's 1775 port is for IAG to sync the user information to CC. IAG's 7443 port is for IAG to submit the asset to CC.
update1.sangfor.net	80(TCP),443(TCP),53(UDP)	Update Server 1 for database update.
update2.sangfor.net	80(TCP),443(TCP),53(UDP)	Update Server 2 for database update.
update3.sangfor.net	80(TCP),443(TCP),53(UDP)	Update Server 3 for database update.

121.46.26.221	80(TCP),443(TCP),53(UDP)	Update Server 4 for database update.
sp1.sangfor.com	80(TCP),443(TCP),53(UDP)	Update Server 1 for System patch
sp2.sangfor.com	80(TCP),443(TCP),53(UDP)	Update Server 2 for System patch
sp3.sangfor.com	80(TCP),443(TCP),53(UDP)	Update Server 3 for System patch
DNS server on CC	53 (UDP)	For Domain name resolve
auth.sea.sangfor.com	80(TCP),443(TCP),53(UDP)	Authentication
upd.sea.sangfor.com	80(TCP),443(TCP),53(UDP)	Configuration Updates
clt.sea.sangfor.com	80(TCP),443(TCP),53(UDP)	Log sync
Ti.sea.sangfor.com	80(TCP),443(TCP),53(UDP)	Threat intelligence
Intelligence.sea.sangfor.com	80(TCP),443(TCP),53(UDP)	Threat intelligence
analysis.sea.sangfor.com	80(TCP),443(TCP),53(UDP)	Threat intelligence
edrsaas.sangfor.com	8083,443,54120,80	Saas-EDR
edragent.sangfor.com	8083,443,54120,80	C/S communication
x.sangfor.com	80(TCP),443(TCP),53(UDP)	Device management
device.sangfor.com	80(TCP),443(TCP),53(UDP)	Device Licensing Server
device.scloud.sangfor.com	80(TCP),443(TCP),53(UDP)	Device management
partner.sangfor.com	80(TCP),443(TCP),53(UDP)	Partner Portal
remote0.scloud.sangfor.com	5000 (TCP, UDP)	Device management